UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/870,610	05/31/2001	Dwip N. Banerjee	AUS9-2001-0361-US1	1787

40412 7590 01/24/2007

IBM CORPORATION- AUSTIN (JVL)
C/O VAN LEEUWEN & VAN LEEUWEN
PO BOX 90609
AUSTIN, TX 78709-0609

EXAMINER	
BAYARD, DJENANE M	
ART UNIT	PAPER NUMBER
2141	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	01/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/870,610
Filing Date: May 31, 2001
Appellant(s): BANERJEE ET AL.

Leslie A. Van Leeuwen
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/25/06 appealing from the Office action mailed 3/03/06.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6189035	Lockhart et al	2-2001
6636972	Ptacek et al	9-2003
6381649	Carlson	4-2002
6321338	Porras et al	11-2001
2003/0110396	Lewis et al	6-2003
2002/0101819	Goldstone	8-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 8 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0110396 to Lewis et al in view of U.S. Patent No. 6,189035 to Lockhart et al.

a. As per claims 1, 8 and 14, Lewis et al teaches a method and apparatus for predicting and preventing attacks in communication networks. Furthermore, Lewis et al teaches providing a test script, the test script including one or more attack simulations (See page 5, paragraph [0061], *the Master infiltrates multiple computer systems and installs the Ddos tools, which are scripts capable of generating large volumes of traffic*); processing the attack simulations included in the test script (See page 5, paragraph [0062]) ; determining whether to change one or more

configuration settings based upon the processing (See page2, paragraph [0018], *one or more of the triggers signal the action-taking means to take the appropriate protective action*) ; changing one or more of the configuration settings based upon determination (See page 2, paragraph [0020], *the protective action are therefore automatically undertaken by the management system*); However, Lewis et al fails to teach receiving a packet from a client computer; identifying the client computer by a source Ip address; calculating a number of packets received using the source Ip address during a time interval, wherein the calculating includes Retrieving a number of packets received that correspond to the source Ip address; and incrementing the number of packets received; comparing the incrementing number of packets received with one or more configuration settings; determining an action from a plurality of actions based on the comparing; and executing the action.

Lockhart et al teaches a method for protecting a network from data packet overload. Furthermore, Lockhart et al teaches identifying the client computer by a source Ip address (See col. 3, lines 25-26, *a determination is made as to whether the incoming data packet has an IP address that is stored in the table*) ; calculating a number of packets received using the source Ip address during a time interval, wherein the calculating includes retrieving a number of packets received that correspond to the source Ip address (See col. 3, lines 65-67 and col. 4, lines 1-50, *a recent packet count is maintained for each IP source that sends data packets to the internal network during a most recent cycle, where a cycle is a time period of several minutes or hours during which the gate 20 receives incoming data packets*); incrementing the number of packets received (See col. 4, lines 3-4, that recent packet count for the present IP source is incremented by one); comparing the incrementing number of packets received with one or more configuration

settings (See col. 4, lines 14-21, *a determination is made as to whether the recent packet count for this particular IP source exceeds a predetermined threshold*) ; determining an action from a plurality of actions based on the comparing; and executing the action (See col. 4, lines 14-26, *if the answer is affirmative, the process advances to where the data packet is discarded* ...).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Lockhart et al in the claimed invention of Lewis et al in order for the number of incoming data packets that are passed to the internal network be limited to a number which the internal network can handle without unduly degrading its operation (See. col. 2, lines 51-56).

b. As per claims 28, 29 and 30, Lewis et al in view of Lockhart et al teaches the claimed invention as described above. Furthermore, Lewis et al teaches wherein at least one of the configuration settings are selected from the group consisting of a number of packets allowed, a time interval, a server port, and an overcount action (See page 4, paragraph [0050]).

3. Claims 5, 11 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0110396 to Lewis et al in view of U.S. Patent No. 6,189035 to Lockhart et al as applied to claims 1, 8 and 14 above, and further in view of U.S. Patent Application No. 2002/0101819 to Goldstone.

a. As per claims 5, 11 and 18, Lewis et al in view of Lockhart et al teaches the claimed invention as described above. However, Lewis et al in view of Lockhart et al fails to teach

receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison.

Goldstone teaches prevention of bandwidth congestion in a denial of service or other internet-based attack. Furthermore, Godlstone teaches receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison (See page 3, paragraph [0038]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison as taught by Goldstone in the claimed invention of Lewis et al in view of Lockhart et al in order for the router to prevent the attacking client from perpetrating further attacks by blocking traffic originating from the attacking client from entering the Internet (See page 3, paragraph [0027]).

5. Claims 21, 23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U U.S. Patent Application No. 2003/0110396 to Lewis et al in view of U.S. Patent No. 6,189035 to Lockhart et al as applied to claim 1, 8 and 14 above and further in view of U.S. Patent No. 6,381649 to Carlson.

a. As per claim 21, 23 and 25, Lewis et al in view of Lockhart et al teaches the claimed invention as described above. However, Lewis et al in view of Lockhart et al fails to teach wherein configuration settings include a first limit and a second limit, the method further comprising: determining that the incremented number of packets exceeds the first limit; processing the packet and sending a notification in response to determining the incremented number of packets exceeds the first limit; receiving a subsequent packet from the client computer; incrementing again the number of packets in response to receiving the subsequent packet; determining that the incremented again number of packets exceeds the second limit; and rejecting the subsequent packet in response to determining that the incremented again number of packets exceeds the second limit.

Carlson et al teaches determining that the number of packets exceeds the first limit; sending a notification in response to determining the number of packets exceeds the first limit; receiving a subsequent packet from the client computer; incrementing the number of packets in response to receiving the subsequent packet; determining that the incremented number of packets exceeds the second limit; and rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit (See col. 7, lines 55-67 and col. 8, lines 1-8).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate determining that the number of packets exceeds the first limit; sending a notification in response to determining the number of packets exceeds the first limit; receiving a subsequent packet from the client computer; incrementing the number of packets in response to receiving the subsequent packet; determining that the incremented number of packets exceeds

the second limit; and rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit as taught by Carlson in the claimed invention of Lewis et al in view of Lockhart et al in order to monitor or police data traffic 9See col. 1, lines 61-64).

6. Claims 22, 24 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0110396 to Lewis et al in view of U.S. Patent No. 6,189035 to Lockhart et al as applied to claim 1, 8 and 14 above and further in view of U.S. Patent No. 6,321338 Porras et al.

a. As per claim 22, 24 and 26, Lewis et al in view of Lockhart et al teaches the claimed invention as described above. However, Lewis et al in view of Lockhart et al fails to teach wherein the configuration settings include a historical' usage corresponding to the client computer, the method further comprising: determining that the number of packets is higher than the historical usage; and sending a notification in response to determining that the number of packets is higher than the historical usage.

Porras et al teaches wherein the configuration settings include a historical' usage corresponding to the client computer, the method further comprising: determining that the number of packets is higher than the historical usage (See col. 6 and 7); and sending a notification in response to determining that the number of packets is higher than the historical usage (See col. 2, lines 54-56).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein the configuration settings include a historical' usage corresponding to the client computer, the method further comprising: determining that the number of packets is higher than the historical usage; and sending a notification in response to determining that the number of packets is higher than the historical usage as taught by Porras et al in the claimed invention of Gupta et al in view of Goldstone and further in view of Lockhart et al in order to identify attacks causing disturbances in more than one network entity 9See col. 2,lines 58-60).

7. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,636972 to Ptacek et al in view of U.S. Patent No. 6,189035 to Lockhart et al and further in view of U.S. Patent Application No. 2002/0059454 to Barrett et al.

a. As per claim 27, Ptacek et al teaches a system and method for building an executable script for performing a network security audit. Furthermore, Ptacek et al teaches executing a test script that includes one or more attack simulations from the client computer, the execution of the test script including (See col. 24, lines 30-42): receiving, at the server computer, one or more packets from the client computer and one or more open socket requests from the client computer (See col. 26, lines 25-37) and the evaluating including: analyzing the performance of the server computer during the simulation; and adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from a group consisting the stored packet limit and the stored socket limit (See col. 6, lines 29-53). However, Ptacek et al

fails to teach deciding a packet threshold for the client computer the deciding including: determining a number of packets received from the client computer during a time interval; incrementing the number of packets received from the client computer; and comparing the number of packets received with a packet limit stored at the server computer; computing an open socket threshold for the client computer, the computing including: determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations.

Lockhart et al teaches a recent packet count is maintained for each IP source that sends data packets to the internal network during a most recent cycle, where a cycle is a time period of several minutes or hours during which the gate 20 receives incoming data packets. In the next step 60, that recent packet count for the present IP source is incremented by one. (18). The present process also maintains a count representing the count of all data packets received... If the answer is negative, the program proceeds to step 70 where a determination is made as to whether the total packet count exceeds its threshold. If the answer is negative, the packet is negative. Otherwise, the packet is discarded. (See col. 3, lines 65-67 and col. 4, lines 1-50).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate deciding a packet threshold for the client computer the deciding including: determining a number of packets received from the client computer during a time interval; incrementing the number of packets received from the client computer; and comparing the number of packets received with a packet limit stored at the server computer as taught by

Lockhart et al in the claimed invention of Ptacek et al in order to determine the packet loss rate calculation over a predetermined window interval (See col. 21, lines 65-67). However, Ptacek et al in view of Lockhart et al fails to teach: determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations.

Barrett et al teaches determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations (See page 1, paragraph [0006]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations as taught by Barrett et al in the claimed invention of Ptacek et al in view of Lockhart et al in order to limit to a number which the internal network can handle the number of incoming packet without unduly degrading its operation (See col. 2, lines 51-56).

(10) Response to Argument

1. **Response to argument presented for Claims 1, 5, 8, 11, 14, 18 and 28-30.**

a) **Configuration Settings**.

As per claims 1, 8 and 14, Appellants argues that the Examiner fails to view Appellants' invention as a whole. Specifically, The Appellant asserts that the Examiner does not view Appellants' "configuration settings" on a consistent basis for each element. However, the Examiner is relying on analogous prior art for the purpose of rejecting the subject matter at issue. Lewis et al teaches a method and apparatus for predicting and preventing imminent network attacks by identifying temporal precursors of such attacks, monitoring future network activity for such precursors, and taking protective action when precursors are detected, thus allowing an attack to be foiled before any damage is done. Lockhart et al teaches a method for protecting a network from being overloaded by an excessive number of data packets that originate form a source in an external network.

The "configuration settings" of Lewis et al are the precursors that are identified events prior to an attack that indicate the onset of an attack. The "configuration settings' of Lockhart et al is the predetermined threshold that should not be exceeded.

Since Lewis et al and Lockhart et al are analogous prior arts and the combined teachings of the references would have suggested the claimed invention to those of ordinary skill in the art, Appellants ' arguments are moot.

b) **Lockhart never teaches changing the predetermined threshold based upon attack simulations.**

In response to Appellants' argument, the Examiner never asserted that Lockhart teaches the predetermined threshold based upon attack simulations. However, Lockhart

"predetermines threshold" changed under attack. Lewis was used as the primary art to teach attack simulation. The Examiner took it into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made to teach claimed invention. The combined teaching Lewis et al and Lockhart et al would have suggested to those of ordinary skill in the art to compare the incremented number of packets received with one or more of the configuration settings in a network under attack simulation.

c) **Lewis's precursor are not based upon a number of packets received from a particular source Ip address**

In response to Appellants' argument, Lewis et al clearly teaches wherein the precursor is based upon "data collected form a communication network during a real or simulation network" (See page 4, paragraph [0047]). The collected data is then analyzed in order to identify the specific precursors of the attack (See page 4, paragraph [0048]). Lewis et al does not specifically teaches how the data is collected (ex. Upon a number of packets received from a particular source Ip address, but Lewis et al teaches wherein data may be collected in any manner known in the art from any aspect of the communications network (See page 4, paragraph 0047). It is well known in the art of networking that data can be collected upon a number of packets received from a particular source Ip address. Lockhart et al was introduced to teach wherein a determination is made as to whether the incoming data packet has an IP address that is stored in the source address table (See col. 3, lines 25-27) and keeping a packet count for each Ip source that sends data packets to the internal network (See col. 3, lines 65-67). Furthermore, Lockhart et al teaches

wherein determination is made as to whether the recent packet count for this particular source exceeds a predetermined threshold (configuration settings). Therefore, it would have been obvious to combine the teaching of Lewis et al of collecting data to determine a precursor with the teaching of Lockhart et al of collecting data based upon Ip address to teach the claimed invention.

2. **Response to arguments presented for Claims 21, 23 and 25**

See arguments above for claims 1, 5, 8, 11, 14, 18 and 28-30.

3. **Response to arguments presented for Claims 22, 24 and 26**

See arguments above for claims 1, 5, 8, 11, 14, 18 and 28-30.

3. **Response to arguments presented for Claim 27.**

3. As per claim 27, Applicant argues Ptacek never teaches or suggests adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from group consisting of the stored packet limit and the stored socket limit. However, Ptacek clearly teaches wherein the CASL is intended simulate attacks against host in order to see if those hosts are vulnerable to attacks of a given nature (See col. 6, lines 29-53). Furthermore, Ptacek teaches wherein one of those simulated attacks will actually send connection requests to each reserved ports (See col. 26, lines 25-37). Furthermore, Ptacek teaches by making it easy to write programs that deal with raw IP packets, CASL allows users to easily simulate protocol-level bugs, including allowing them to test their machines for potential vulnerability to such bugs (See col. 6, lines 54-57) and simple CASL code, which will

not only run on the machines they need to run on, but also work exactly how they need to work (See col. 7, lines 1-2).

It would have been obvious to one with ordinary skill in the art to conclude that Ptacek is doing simulated network attack in order to test the vulnerabilities of the network and to adjust the configuration setting.

For the above reasons, it is believed that the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

Djenane Bayard D.B.

Conferees:

Rupal Dharia (SPE)

Kenneth Coulter (Primary Examiner)

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100